Table of Contents

1.0 GENERAL

1.1 *SUMMARY*

The Office of Technology Services (OTech) provides Secure Sockets Layer (SSL) certificates on leased equipment in the Application Hosting environment within the data center and external OTech customers. These certificates are a nonproprietary protocol for securing data communications across computer networks and will provide data encryption while in transit for TCP/IP connections.

Included in the offering, where OTech manages Customer web servers, are certificate procurement, installation, and administration. Staff performs these tasks according to internal procedures and standard configurations. OTech will provide certificate procurement services for all other Customer systems; including Application Hosted web servers unmanaged by OTech.

OTech provides version(s) of certificates in accordance with current certificate industry standards. Certificates are offered on both dedicated and virtual server platform configurations that support standard V3 certificates. OTech is authorized to offer certificates only for the following domains:

.ca.gov
.cahwnet.gov
.state.ca.us

OTech does not provide self-signed certificates.

This document provides guidance in selecting SSL secure certificates.

1.2 *REFERENCES*

Items referenced here are support information provided in this document:

	IDENTIFIER	DATE	TITLE
	01.05.884	2012	Secure Certificate Submittal
	n/a	2013	Environment Submittal
	n/a	2013	Environment Submittal Instructions
	4000	2011	OTech Software Version Support Policy
	4000	2011	OTech Software Version Support Procedure
	Web Site	NA	OTech Contact Information

1.3 *SUBMITTALS*

1.3.1 General

OTech is available to advise and assist customers in formulating IT designs that will leverage available service offerings. Contact your Account Manager to engage architectural/engineering and design consulting services. Additional charges may be incurred.

The OTech requires the following method be used for work requests:

Item	Request Method
Quotes & Billable Service (new or changes to existing services)	OTech Customer Service System (CSS) Request
Modifications to Existing Systems	OTech Service Desk or Remedy Service Request
Technical Problems	OTech Service Desk or Remedy Incident
Security Related Issues/Incidents	OTech Service Desk
SSL Submittal Questions	Certificate_Services@state.ca.gov

Include the Customer's name, contact information and associated project name on forms, documents, and requests submitted to OTech.

1.3.2 Service Request Criteria

A completed Secure Certificate Submittal is required for new certificates and renewals prior to the start of work. To aid in the preparation of providing this technology, all information must be included in the OTech Service Request. Customer Service System (CSS).

This Submittal is to be revised at appropriate intervals providing for expeditious and practicable execution of the work. Revised submittal(s) must indicate changes, if any.

1.4 *EXPECTATIONS*

1.4.1 OTech

OTech manages contract and licensing for certificate management software and serves as liaison between the customer and certificate vendor for technical issues.

OTech will notify Customers of upcoming renewals in accordance with the contact information provided on the Secure Certificate Submittal. Technology products must be within vendor supported versions to sustain availability and integrity.

OTech will obtain certificate backups for web servers managed by OTech.

OTech follows change management practices. Change requests are recorded in the OTech Remedy Service Request system, as a Change Request (CRQ). Contact your OTech account managers for current change procedures.

1.4.2 Customer

Customers are expected to notify Certificate_Services@state.ca.gov of changes to certificate contact(s).

Certificates purchased for systems outside of Application Hosting where OTech is managing the web server, must be installed and verified by the Customer.

Customers are to determine and submit technology details required to meet their certificate needs.

1.5 *SCHEDULING*

OTech's goal is to provide timely, comprehensive and economical technology service manner. Customers promote this goal by promptly providing information requested, and by keeping the OTech Account Manager / Project Manager informed of technology project status.

Completed and approved service requests for new certificates will typically be available 3 to 5 business days after the normal service request processing time. Renewals are not processed by OTech until a week prior to the current certificate expiration date. If they are needed earlier please note the requested delivery date on the service request. Certificates will expire at 1700 on the final day of the active certificate.

Delays in the service request process, server readiness to obtain the certificate, or the lack of or validity of the CSR file will impact the timeliness of the certificate delivery.

A 25 calendar day window immediately following the delivery of a certificate from OTech is provided for certificate testing, revocation or changes.

1.5.1 Maintenance

Not Used

1.5.2 Change Management Schedule

Change proposal / requests follow the established OTech Change Management process. Work performed during scheduled maintenance periods is subject to the OTech Change Management Schedule. Changes require 2-week prior notification.

Shorter periods may not always be expedited; additional charges may be incurred for expedited change requests.

1.6 *DEFINITIONS*

Term, phrase, abbreviation	**Definition**
SSL	Secure Sockets Layer
SAN	Subject Alternative Name
CSR	Certificate Signing Request
DNS	Domain Name Service
HTTPS	Hypertext Transfer Protocol over SSL
TCP/IP	Transmission Control Protocol/Internet Protocol

2.0 PRODUCTS

2.1 *MANUFACTURER*

Comodo Group, Inc.

2.1.1 Unit Pricing

Certificates are available in one or two year units. Expedited certificate requests are subject to expedite fee(s).

Certificate fees will vary depending on the number of servers and of URLs for which the certificate applies. For example, a 2-year SAN certificate with 3 URLs for 4 load balanced servers will cost $6,000. This is ($500 * 3 * 4). OTech obtains the "per URL" number from item #1 and the "per server" from item #3 on the Secure Certificate Submittal.

Certificate Pricing	1 Year	2 Year
Certificate Fee (per URL/per server)	$250.00	$500.00
Administration Fee	$130.00	
OTech Installation Fee	$130.00	

One certificate *administration* fee is applied per domain name and per SAN certificate.

Certificate *installation* fees are applied per server, per domain name. This is in addition to the certificate administration fee. Installation fees only apply when OTech performs the certificate installation(s).

If certificate revocation occurs within the 25 calendar day testing window, the cost of the certificate license will be reimbursed however the administration and installation fee(s) will not. Contact your OTech Account Manager for information regarding the Credit Reimbursement process.

2.2 *PLATFORM*

Certificates are available on servers running the following:

Microsoft Internet Information Server (IIS)

Apache HTTP Server

For additional platform options contact CIOCert_Request_DG@state.ca.gov.

2.3 *PRODUCT FORMATS*

Certificates are available from OTech in the following formats:

PKCS#7 (.p7b file)

X.509 (.cer file)

Within Application Hosting where OTech manages the web servers, OTech will also convert the certificate into PFX (.pfx file) format for use on load balancers and proxy devices.

3.0 EXECUTION

3.1 *SECURITY*

SSL certificates should be used if information in transit between different computer networks needs to be protected. Common certificate applications include:

1. Encrypting personally identifiable information (PII) while in transit.
2. Complying with required regulatory privacy or security requirements.

Configuration changes made outside the scope delineated above and needing intervention, correction, or troubleshooting by OTech staff may incur additional charges.

3.2 *QUALITY CONTROL*

1. If a web server does not already have a free, unique, IP address, a unique address will need to be requested. This request is made to your hosting location, example: OTech or external host site.
2. New domain names must be approved by Web Services and must comply with federal General Services Administration (GSA) guidelines.
3. A new web site typically needs a new DNS entry request for the new domain name.
4. When using HTTPS (port 443) confirm the network port opening is permitted to allow this traffic across applicable network devices (e.g., proxies, routers).
5. Up to 100 domain names may be applied to a single SAN certificate.

Prohibited

1. Top-level domain name endings in: .com .net .biz .org
2. Use of top-level domain name containing "/" symbol. Examples: "xyz.ca.gov/secure" or "zyx.ca.gov/finance"

3.2.1 OTech Responsibilities

1. Contract management
2. Engage Comodo Group, Inc. services as necessary for problem resolution involving the certificate
3. Review and recommend optional certificate application that may better meet requirements in accordance with the project and/or 1.3 - SUBMITTALS
4. Review submittal for completeness and approve prior to beginning work
5. Notify Customer of submittal flaws, if any
6. Send Customer 30,60,90 day automated certificate expiration notifications

Additionally within Application Hosting where OTech manages the web server:

7. Certificate installation, verification and support
8. Coordination with other, internal OTech teams regarding proxy/load balancer certificate installation

9. Assist customer in specifying design, if applicable, in accordance with information provided in 1.3 - SUBMITTALS

3.2.2 Customer Responsibilities

1. Initiate renewal of certificate prior to its expiration. Refer to 1.5 – SCHEDULING
2. Provide complete and timely submittal; refer to 1.3 - SUBMITTALS information
3. Notify OTech of changes that impact the certificates use
4. Document certificates within the application architecture and keep it current

3.3 *SUPPORT AVAILABILITY*

Core business hours for technical support are Monday through Friday 0800-1700. State holidays and mandated schedule alterations are observed and may impact staff availability.

3.4 *INSTALLATION*

3.4.1 OTech Responsibilities within Application Hosting where OTech manages the Web Server

1. Installation of certificates will be in accordance with the 1.3 - SUBMITTALS and current industry certificate standards
2. Retain certificate root authority
3. Install certificate renewals
4. Communicate certificate installation

3.4.2 Customer Responsibilities include but are not limited to

1. Notify OTech of changes that impact the certificates use
2. Document certificates within the application architecture and keep it current
3. Test third party application functionality with the certificate
4. Additional charges for OTech intervention, troubleshooting and correction of unauthorized changes that impact OTech's responsibilities of the certificate.
5. Test system upon certificate modifications. Only notify OTech of adverse test results
6. The Customer is responsible for conversion into formats not listed in Section 2.3 - *PRODUCTS FORMATS*.

3.4.3 Customer Responsibilities for certificates outside of OTech managed Web Servers

This includes unmanaged web servers within Application Hosting.

1. Installation, Certificate Signing Request (CSR) generation, and certificate configuration
2. Certificate backups